Abstract of the Disclosure:

A method for authentication and identification uses different keys for the prover and the verifier, but on the other hand dispenses with the utilization of long number modulo arithmetic by the use of simple basic components such as, for example, arithmetic operations in finite bodies GF(2^n). A private key is stored in the prover, so that the latter can receive, in encrypted form, data elements generated as random elements and can itself utilize them again as key for an authentication method of a data set to be transmitted. The verifier receives the authenticator thus formed and checks it. If the data set is generated by the verifier and transmitted to the prover, then this method can serve for the identification of the prover. The method is particularly advantageous in the area of smart cards, since there the required space in the hardware implementation can be considerably reduced.

REL/nt